IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

MATTHEW TINCHER, individually and on behalf of all others similarly situated, Plaintiff, v. QRS, Inc., Defendant.	**Case No.** **CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF** **JURY DEMAND**

Plaintiff MATTHEW TINCHER ("Plaintiff") brings this Class Action Complaint against QRS, Inc. ("Defendant" or "QRS"), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") involving QRS, a healthcare technology services vendor that hosts an electronic patient portal for various healthcare provider clients.

2. QRS failed to reasonably secure, monitor, and maintain the Protected Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively, "Sensitive Information") stored on its patient portal. As a result, Plaintiff and approximately 319,000 current and former patients of healthcare providers that utilized QRS's services suffered present injury and damages in the form of identity theft, loss of value of their Sensitive Information, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, after learning of the Data Breach, Defendant waited roughly two months

to notify Plaintiff and Class Members of the Data Breach and/or inform them that their Sensitive Information was compromised. During this time, Plaintiff and Class Members were unaware that their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. By obtaining, collecting, using, and deriving a benefit from the Sensitive Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiff brings this action on behalf of all persons whose Sensitive Information was compromised as a result of Defendant's failure to take reasonable steps to protect the Sensitive Information of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII and PHI of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

6. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, concrete and imminent injury. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited

to lost time; and (iv) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI; (iv) the invasion of privacy; (v) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Member's PII and PHI; and (vi) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII and PHI.

7. Plaintiff seek to remedy these harms, and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

8. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Matthew Tincher

9. Plaintiff Matthew Tincher is a resident and citizen of Kentucky, currently residing in Frankfort, Kentucky. Plaintiff Tincher received a "Notice of Data Breach" letter dated October 22, 2021, on or about that date. The letter notified Plaintiff Tincher that an unauthorized third party gained accessed to Defendant's server that contained Plaintiff's full name, Social Security number, date of birth, patient number, and portal username. Upon information and belief, based on the criminal hacking activity that targeted Plaintiff's and Class Members' Sensitive Information, the time frame of the breach over three days, and Plaintiff Tincher's experience of actual identity theft shortly after the breach, it is more likely than not that his Sensitive Information was exfiltrated and stolen during the Data Breach.

10. Defendant obtained and continues to maintain Plaintiff's Sensitive Information and has a continuing legal duty and obligation to protect that Sensitive Information from unauthorized

access and disclosure. Defendant required the Sensitive Information from Plaintiff when Plaintiff received medical treatment from one of Defendant's customers. Plaintiff, however, would not have entrusted his Sensitive Information to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's Sensitive Information was compromised and disclosed as a result of the Data Breach.

Defendant QRS, Inc.

11. Defendant QRS, Inc. is a Tennessee corporation with its principal office located at 2010 Castaic Ln, Knoxville, TN 37932-1557. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The total amount of damages incurred by Plaintiff and the Class in the aggregate exceeds the $5 million jurisdictional minimum of this Court. Upon information and belief, the number of class members is in the hundreds of thousands, many of whom have different citizenship from Defendant QRS, including the named Plaintiff here. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

13. This Court has jurisdiction over the Defendant because QRS, Inc. operates and is incorporated in this District, and the server implicated in this Data Breach is likely based in this District.

14. Venue is proper in this Court under 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is based in this District, maintains Class Members' PII and PHI in the District and have caused harm to Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Background

15. Defendant is a health care support company which offers clients software "to streamline their scheduling, charting, imaging, billing, patient engagement, encounter documentation, data security, and more."[1] "Since October 1993, the company has focused [its] efforts toward developing products to provide solutions for health care providers and medical services organizations."[2]

16. Among other services, QRS hosts the electronic patient portal for certain healthcare providers. The "patient portal" is where the patients of healthcare providers that utilize QRS's services input their Sensitive Information for their doctors and other medical care providers. In the ordinary course of interacting with the QRS patient portal, patients are required to provide sensitive PII, such as names, dates of birth, Social Security numbers, addresses, phone numbers, and email addresses, as well as sensitive PHI, such as medical histories, treatment information, medication or prescription information, provider information, and health insurance information.

17. Because of the highly sensitive and personal nature of the information QRS acquires and stores with respect to its healthcare provider clients' patients, and by operation of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), QRS has a legal duty to keep patient PHI safe and confidential.

18. Upon information and belief, pursuant to a "software services agreement" contract between QRS and its clients, Defendant maintained personal information related to its clients' patients on its computer systems as a result of the services it provided to its clients.

19. Upon information and belief, pursuant to that same contract between QRS and its

[1] https://www.qrshs.com/about/ (last visited December 19, 2021).
[2] *Id.*

clients, the parties specifically contracted and agreed that all data and information belonging to the patients of QRS's clients shall be held by QRS in the strictest confidence. QRS further agreed not to disclose such information to any third party without the express prior written consent of its clients or unless required by applicable law or court order.

20. Upon information and belief, that same contract between QRS and its clients expressly acknowledges that QRS will be collecting and holding HIPAA protected PHI, and that QRS is bound to follow the HIPAA Privacy Rule with regard to the PHI it collects on behalf of its clients who are HIPAA covered entities.

21. Defendant QRS, acting as a business associate and vendor of its healthcare provider clients, held the patient information collected by its clients at its servers located in Knoxville, Tennessee.

22. The patient information held by Defendant in its computer systems and networks included the Sensitive Information of Plaintiff and Class Members.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Sensitive Information, QRS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Sensitive Information from disclosure.

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Sensitive Information.

The Data Breach

25. On August 26, 2021, QRS discovered that an unauthorized actor accessed a QRS dedicated patient portal server and potentially acquired certain personal information stored on that specific server.

26. Defendant's investigation subsequently determined that the attacker first gained access to the server on August 23, 2021.

27. Between August 23 and August 26, 2021, the attacker accessed, and likely acquired, files on the server containing Sensitive Information, including names, addresses, dates of birth, Social Security numbers, patient identification numbers, health portal usernames, and medical treatment or diagnosis information.

28. QRS first notified its health provider clients of the incident. On October 22, 2021, on behalf of QRS's clients, QRS began sending written notifications to individuals whose personal information was compromised in the Data Breach and for whom QRS had contact information.

29. On October 22, 2021, Defendant also disclosed the Data Breach to the U.S. Department of Health and Human Services' Office for Civil Rights, including the fact that 319,778 individuals had their Sensitive Information compromised in the Data Breach.[3]

30. Plaintiff's and Class Members' Sensitive Information was accessed and stolen in the Data Breach.

31. Plaintiff further believes his PII and PHI, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type

32. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited December 19, 2021).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

33. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you

know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[4]

34. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

[4] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 11, 2021).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[5]

35. Given that Defendant was storing the PII and PHI of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

36. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII and PHI of an undisclosed amount of current and former patients, including Plaintiff and Class Members.

[5] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

Defendant Acquires, Collects, and Stores the PHI & PII of Plaintiff and Class Members

37. Defendant has historically acquired, collected, and stored the PII and PHI of Plaintiff and Class Members.

38. As part of receiving treatment from Defendant's clients, Plaintiff and Class Members, are required to give their sensitive and confidential PHI and PHI to Defendant. Defendant retains this information.

39. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

41. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII and PHI of Plaintiff and Class Members.

42. Defendant's policies on its website include promises and legal obligations to maintain and protect PII and PHI, demonstrating an understanding of the importance of securing PII and PHI.

43. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

44. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

Defendant Knew or Should Have Known of the Risk Because the Healthcare Sector is Particularly Susceptible to Cyber Attacks

45. Defendant knew and understood unprotected or exposed PII and PHI in the custody of healthcare service companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII and PHI through unauthorized access.

46. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[6] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[7] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.[8]

47. Healthcare related data breaches continue to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident within the previous 12 months, and most of these known incidents being caused by "bad actors," such as cybercriminals.[9] "Hospitals have emerged

---

[6] *See* Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/ (last visited Nov. 11, 2021).
[7] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Nov. 11, 2021).
[8] *See id.*
[9] *See 2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Nov. 11, 2021).

as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

48. As a healthcare service provider, Defendant knew or should have known the importance of safeguarding PII and PHI entrusted to it, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take reasonable cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

49. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

50. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Personal Information can be sold at a price ranging from $40 to $200,

[10] *See* Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Nov. 11, 2021).
[11] 17 C.F.R. § 248.201 (2013).
[12] *Id*.

and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

51. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

52. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

53. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

---

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Nov. 11, 2021).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 11, 2021).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 11, 2021).

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 11, 2021).

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, name, and date of birth.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

56. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

57. The fraudulent activity resulting from the Data Breach may not come to light for years.

58. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Nov. 11, 2021).

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 11, 2021).

from data breaches cannot necessarily rule out all future harm.[19]

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed, PII and PHI, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. In the breach notification letter, Defendant made an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members.

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 11, 2021).

64. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiff and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant's Conduct Violates HIPPA

65. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities, including Defendant, must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[20]

66. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI—the type of data Defendant failed to safeguard. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

67. Defendant's Data Breach resulted from a combination of insufficiencies demonstrating Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to

[20] *See* HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?, available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last visited Nov. 11, 2021).

allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii);

e. Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502, *et seq.*; and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

Plaintiff Tincher's Experience

68. Plaintiff Tincher received medical treatment from Lexington Heat Specialists, which is one of Defendant's clients. Plaintiff's Sensitive Information was entrusted to Defendant in connection with these services. At the time of the Data Breach, Defendant retained Plaintiff's Sensitive Information in its system.

69. Plaintiff received Defendant's Notice of Data Breach, dated October 22, 2021, on or about that date. The notice stated that Plaintiff's full name, Social Security number, date of birth, patient number, and portal username were among the information accessed or acquired during the Data Breach.

70. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice of the Data Breach and self-monitoring his accounts and credit statements. He has also spent time changing passwords and ordering new credit cards. This time has been lost forever and cannot be recaptured.

71. Mr. Tincher has also been targeted with scams involving IRS and medical billing in the form of increased spam emails, texts and robocalls.

72. Shortly after the Data Breach, Mr. Tincher experienced actual identity theft, including more than ten unauthorized charges on his between his bank account and credit card. This resulted in trips to the bank, with gas charges and consumption and mileage on his car, and additional time spent completing paperwork and discussing the issues with the bank for resolution.

73. In response, and in an effort to further mitigate his risk of future identity theft, Plaintiff incurred out of pocket expenses downloading a mobile phone application (MaxRewards) to monitor his credit card and track all expenses. This mobile application costs $14.99 per month. He also signed up for identify theft protection on Experian, which costs an additional $14.99 per month.

74. Plaintiff is very careful about sharing his Sensitive Information. He has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. He is unaware of any other data breach that compromised the Sensitive Information disclosed and likely acquired in the Data Breach.

75. Plaintiff stores any documents containing his Sensitive Information in a safe and secure location or destroys documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

76. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII and PHI – forms of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

77. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his and his family's privacy.

78. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his Sensitive Information resulting from his PII and PHI being placed in the hands of unauthorized criminal third parties.

79. Plaintiff has a continuing interest in ensuring that his Sensitive Information, which upon information and belief remains in Defendant's possession, is adequately protected and safeguarded from future breaches.

80. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security Number and medical information, being placed in the hands of criminal third parties.

81. Defendant obtained and continues to maintain Plaintiff's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure. Defendant required Plaintiff's PII and PHI when Plaintiff received medical treatment from his healthcare provider. Plaintiff, however, would not have entrusted his PII and PHI to his healthcare provider and/or Defendant had he known that Defendant would fail to maintain reasonable data security. Plaintiff's PII and PHI was compromised and disclosed as a result of the Data Breach.

82. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

83. Plaintiff brings this suit on behalf of himself and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

> **All persons QRS identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

84. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

85. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, but are reported to be at least 319,000. The identities of Class Members are ascertainable through QRS's records, Class Members' records, publication notice, self-identification, and other means.

86. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether QRS unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Sensitive Information;

b. Whether QRS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether QRS's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether QRS's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether QRS owed a duty to Class Members to safeguard their Sensitive Information;

f. Whether QRS breached its duty to Class Members to safeguard their Sensitive Information;

g. Whether computer hackers obtained Class Members' Sensitive Information in the Data Breach;

h. Whether QRS knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of QRS's misconduct;

j. Whether QRS's conduct was negligent;

k. Whether QRS's conduct was per se negligent, and;

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties,

punitive damages, and/or injunctive relief.

87. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's Sensitive Information, like that of every other Class member, was compromised in the Data Breach.

88. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

89. **Predominance.** QRS has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

90. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for QRS. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

91. QRS has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a

Class-wide basis.

92. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether QRS owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Sensitive Information;

b. Whether QRS's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether QRS's failure to institute adequate protective security measures amounted to negligence;

d. Whether QRS failed to take commercially reasonable steps to safeguard consumer Sensitive Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

93. Finally, all members of the proposed Class are readily ascertainable. QRS has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by QRS.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

94. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 93.

95. QRS knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Sensitive Information, and had a duty to exercise reasonable care in safeguarding,

securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

96. QRS had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Sensitive Information.

97. QRS had a duty to employ reasonable security measures and otherwise protect the Sensitive Information of Plaintiff and Class Members pursuant to Tenn. Code. §§ 47-18-2105 to 2107 (2005).

98. QRS had a duty to employ reasonable security measures and otherwise protect the Sensitive Information of Plaintiff and Class Members pursuant to Tenn. Code. § 47-18-2110 (2018).

99. QRS had a duty to employ reasonable security measures and otherwise protect the Sensitive Information of Plaintiff and Class Members pursuant to Tenn. Code. § 39-14-150(G).

100. QRS systematically failed to provide adequate security for data in its possession.

101. QRS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Sensitive Information within QRS's possession.

102. QRS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Sensitive Information.

103. QRS, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Sensitive Information within QRS's possession might have been compromised and precisely the type of information compromised.

104. QRS's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Sensitive Information to be compromised.

105. As a result of QRS's ongoing failure to notify Plaintiff and Class Members regarding what type of Sensitive Information has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

106. QRS's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Sensitive Information.

107. As a result of QRS's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Sensitive Information, which is still in the possession of third parties, will be used for fraudulent purposes.

108. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

109. In failing to secure Plaintiff's and Class Members' Sensitive Information and promptly notifying them of the Data Breach, QRS is guilty of oppression, fraud, or malice, in that QRS acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

110. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling QRS to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

111. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 110.

112. Pursuant to Section 5 of the FTC Act, and Tennessee law (e.g., Tenn. Code. §§ 47-18-2105 to 2107 (2005)), QRS was required by law to maintain adequate and reasonable data and

cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Sensitive Information.

113. Plaintiff and Class Members are within the class of persons whom Section 5 of the FTC Act and Tenn. Code. §§ 47-18-2105 to 2107 were among the specific class of people that these statutes were designed to protect.

114. QRS breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

115. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Sensitive Information in compliance with applicable laws would result in an unauthorized third-party gaining access to QRS's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Sensitive Information.

116. Plaintiff's and Class Members' Sensitive Information constitutes personal property that was stolen due to QRS's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

117. QRS's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Sensitive Information and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of QRS's conduct. Plaintiff and Class Members seek damages and other relief as a result of QRS's negligence.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

118. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 117.

119. Plaintiff and Class Members maintain a privacy interest in their Sensitive Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

120. Plaintiff and Class Members' Sensitive Information was contained, stored, and managed electronically in QRS's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, unique identification numbers, medical histories, and financial records that were only shared with QRS for the limited purpose of obtaining and paying for healthcare, medical goods and services.

121. Additionally, Plaintiff's and Class Members' Sensitive Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Sensitive Information for fraud, identity theft, and other crimes without their knowledge and consent.

122. QRS's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Sensitive Information is offensive to a reasonable person. QRS's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their Sensitive Information was stored and disclosed private facts about their health into the public domain.

123. Plaintiff and Class Members have been damaged by QRS's conduct, by incurring the harms and injuries arising from the Data Breach now and in the future.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

124. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 123.

125. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII and PHI that Plaintiff and the Class provided to Defendant.

126. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

127. Plaintiff and the Class provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

128. Plaintiff and the Class also provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

129. Defendant voluntarily received in confidence Plaintiff's and the Class's PII and PHI with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

130. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

131. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

132. But for Defendant's disclosure of Plaintiff's and the Class's PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class's PII and PHI as well as the resulting damages.

133. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII and PHI.

134. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of current and former patients and their beneficiaries and dependents; and (viii) present and future costs in terms

of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

135. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

136. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 135.

137. Defendant benefited from receiving Plaintiff's and Class Members' PII and PHI by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

138. Defendant also understood and appreciated that Plaintiff's and Class Members' PII and PHI was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

139. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII and PHI to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII and PHI. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII and PHI held by Defendant.

140. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

141. Defendant failed to provide reasonable security, safeguards, and protections to the PII and PHI of Plaintiff and Class Members.

142. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

143. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

144. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

145. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

SIXTH CAUSE OF ACTION
VIOLATIONS OF THE TENNESSEE CONSUMER PROTECTION ACT OF 1977
Tenn. Code Ann. § 47-18-101, *et seq*.

146. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 145.

147. Plaintiff brings this claim on behalf of himself and the Class set forth above.

148. Plaintiff brings this cause of action pursuant to Federal Rule of Civil Procedure 23, which, procedurally, displaces any state procedural statutory ban on class actions under Tennessee's Consumer Protection Act ("TCPA").

149. Plaintiff and Class Members are "natural persons" and "consumers" within the meaning of Tenn. Code § 47-18-103(2).

150. QRS is engaged in "trade" or "commerce" or "consumer transactions" within the meaning Tenn. Code § 47-18-103(9).

151. The TCPA prohibits "unfair or deceptive acts or practices affecting the conduct of any trade or commerce." Tenn. Code § 47-18- 104. 159. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard Sensitive Information;

b. failing to disclose that their computer systems and data security practices were inadequate to safeguard Sensitive Information from theft;

c. continued gathering and storage of Sensitive Information and other personal information after Defendant knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach;

d. making and using false promises about the privacy and security of Sensitive Information of Plaintiff and Class Members, and;

e. continued gathering and storage of PII and other personal information after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident.

152. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, HIPAA, and Tenn. Code Ann. § 47-18-101, et seq.

153. The foregoing deceptive acts and practices were directed at consumers.

154. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of Sensitive Information.

155. QRS's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which

reasonable persons, including Plaintiff and members of the Class, would attach importance to in making their decisions and/or conducting themselves regarding the services received from QRS.

156. Plaintiff and Class members are consumers who made payments to the clients of QRS for the furnishing of healthcare services that were primarily for personal, family, or household purposes.

157. QRS engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of employment benefit services to consumers, including Plaintiff and Class Members.

158. QRS engaged in, and its acts and omissions affect, trade and commerce, or the furnishing of services in the State of Tennessee.

159. QRS's acts, practices, and omissions were done in the course of QRS's business of furnishing healthcare providers with patient portal and other services in the State of Tennessee.

160. As a direct and proximate result of QRS's multiple, separate violations of the Tennessee CPA, Plaintiff and the Class Members suffered damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Sensitive Information, which remains in QRS's possession and is subject to further unauthorized disclosures so long as QRS fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession, and; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

161. Also, as a direct result of QRS's violation of the Tennessee CPA, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering QRS to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

162. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from QRS's unfair, deceptive, and unlawful practices. QRS's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

163. QRS knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

164. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

165. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages, three times actual damages, and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully submitted,

*/s/ Daniel Parish*_____

Daniel V. Parish, BPR No. 027452
Wolff Ardis, P.C.
5810 Shelby Oaks Drive
Memphis, Tennessee 38134
Telephone (901) 763-3336
Fax (901) 763-3376
dparish@wolffardis.com

Joseph M. Lyon (*pro hac vice* forthcoming)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Terence R. Coates (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Counsel for Plaintiff and the Class